Exhibit H ORCA Agency Security Plan

1.0 DEFINITIONS

Capitalized terms used in this Exhibit are defined in Section 3 of the Interlocal Agreement to which this attached and as specified below.

1.1 Agency Security Committee means the committee established by the Joint Board under this Agency Security Plan.

1.2 Agency Security Administrator means the individual designated by an Agency to 1) act as the single point of contact for an Agency related to system security matters; and 2) act as the staff responsible for assessing Agency staff system access levels, authorizing this level of access and submitting a request to the Contractor to issue appropriate system access passwords.

1.3 Contractor means ERG Transit Systems (USA) and its employees, subcontractors, successors and assigns.

1.4 CDRL 31 Security Plan means the Contract Deliverable per Contract No. 229944 which describes the Contractor's plan for assuring system security as required under said Contract.

1.5 FTP means Fare Transaction Processor. The device with which the customer most commonly interacts to conduct a fare transaction.

1.6 Interlocal Agreement means *The Interlocal Cooperation Agreement for Design, Implementation, Operation, and Maintenance of the Regional Fare Coordination System, as amended and restated.*

1.7 Lead Agency means an Agency authorized to enter into agreements with Retail Revalue Entities or Business Accounts.

1.8 User means any individual or entity authorized by an Agency to access data and equipment that is part of the ORCA System.

1.9 PCI Data Security Standard or PCI-DSS refers to Payment Card Industry Data Security Standard developed by Visa® and MasterCard to create common industry security requirements.

1.10 Personally Identifying Information" (PII) means the following information when collected by the Agencies under the ORCA Program: a natural person's name; and, if combined with said name, the address, telephone number, e-mail address, date of birth, Regional Reduced Fare Permit-related information, photo, and check/debit card/credit card information.

1.11 Regional Fare Coordination System (RFCS) means the common, non-cash fare system developed and operated by the RFC Contractor to enable customers of public transportation to use the same fare payment media throughout the Agencies' service areas.

1.12 Regional Program Administrator means the employee of the Regional Program Administration Agency who is approved by, and reports to, the Joint Board during the Operating Phase.

1.13 Regional Security Administrator means the employee of the Regional Program Administration Agency who provides regional coordination and staff support to the Agency Security Committee.

1.14 Security Incident means a violation of the Agency Security Plan, the CDRL 31 Security Plan, individual Agency security policies and procedures, unauthorized or attempted unauthorized access to non-public elements of the RFCS, unwanted disruption of systems, introduction of malware, or changes to hardware and software not authorized by the Agencies.

1.15 Security Review Board or SRB means the group of Contractor staff and Agency representatives responsible for security-related activities as provided in the CDRL 31 Security Plan.

2.0 AGENCY SECURITY COMMITTEE AND REGIONAL SECURITY ADMINISTRATOR

2.1 The Agencies shall form an Agency Security Committee consisting of at least one representative from each Agency. Each Agency shall have one vote on the Agency Security Committee even if it has more than one representative.

2.2 Each Agency shall assign up to two representatives to the Agency Security Committee, which shall provide representation in (1) risk and business management and (2) technology and information technology.

2.3 The Agency Security Committee shall have the following general responsibilities, as well as other responsibilities as may be specifically set forth in this Agency Security Plan or as directed by the Joint Board:

- 2.3.1 Annual risk assessment at the Agency level.
- 2.3.2 Coordination of an annual review of each Agency's compliance with the Security Plan requirements.
- 2.3.3 Security Incident coordination between the Agencies and authorization of responses within policies approved by the Joint Board.
- 2.3.4 Annual review of CDRL 31 Security Plan and coordination of proposed changes.
- 2.3.5 Annual review and comment of the external security audit of Contractor's Concord, California facility.
- 2.3.6 Development of security awareness guidelines.

2.4 The Agency Security Committee shall prepare and submit to the Joint Board such proposed work plans, policies, procedures and other materials as may be directed by the Joint Board or as may be recommended by the Agency Security Committee. The Agency Security Committee shall not have final decision-making authority on any Agency Security matters except as may be specifically authorized by the Joint Board.

2.5 The Agency Security Committee shall select one Agency representative to serve as its chair and another Agency representative to serve as its vice-chair. The Committee shall

determine when, where and the frequency of its meetings, and take other necessary and appropriate actions to fulfill its responsibilities under this Agency Security Plan.

2.6 The Agency Security Committee shall not in itself be part of the Security Review Board. However, Agency representatives to the Agency Security Committee may also serve as Agency representatives to the Security Review Board.

2.7 Each member of the Agency Security Committee shall represent and coordinate with others within that member's own Agency on security matters.

2.8 The Regional Program Administration Agency shall designate an employee to serve as Regional Security Administrator, which employee shall not have other RFCS duties and responsibilities except as may be specifically authorized by the Joint Board. The Regional Security Administrator will provide staff support to the Agency Security Committee.

3.0 AGENCY SECURITY PRACTICES

3.1 Agency Risk Assessment

3.1.1 The Agency Security Committee shall conduct an annual risk assessment. This process will include evaluation of the risks and threats identified in CDRL 31 Security Plan as they pertain to Agencies, and recommend revisions to the document due to identified new risks, changes in the RFCS or environment. The Agency Security Committee will also review the Agency controls defined in this Agency Security Plan and review the controls for adequacy in mitigating the risks when appropriate.

3.1.2 Each Agency shall fully cooperate and participate in the annual security review approved by the Joint Board, including self-assessments and any PCI-DSS or other security reviews conducted by outside consultants, insurance providers or other parties. Such cooperation includes but is not limited to allowing access to an Agency's facilities and records.

3.2 Security Plans

3.2.1 Agencies may request an exception to the requirements in this Agency Security Plan by submitting a written request to the Chair of the Agency Security Committee describing the request and describing the potential risks. The Committee will evaluate requested exceptions on the basis of overall risk to the RFCS and submit its recommendations to grant or deny the requested exceptions to the Joint Board for its consideration and action. The Committee shall document in writing all granted or denied exception requests.

3.2.2 The Agency Security Committee's annual review of the security controls in the Agency Security Plan will identify and recommend any potential changes to the Agency Security Plan that need to be made in order to adequately mitigate identified risks that are managed by the Agencies.

3.2.3 The Agency Security Committee shall work with the ORCA Operations Manager in monitoring the Contractor's annual external security audit and shall conduct an annual review of the CDRL 31 Security Plan. This process will identify and recommend any potential changes to the CDRL 31 Security Plan that need to be made in order to adequately mitigate identified risks that are managed by the Contractor.

3.3 Organization of Agency Security and Governance

3.3.1 Agencies shall be responsible for complying with laws, regulations, and contractual obligations that apply to them directly. In cases where implementing controls and demonstrating compliance involves elements of the RFCS that are operated and maintained by the Contractor, the SRB will be the body responsible for identifying a compliance strategy that includes all necessary stakeholders and may include updates to CDRL 31 Security Plan, the Agency Security Plan or both.

3.3.2 Agencies shall coordinate all external audits and reviews of the RFCS with the SRB in order to identify possible duplication of efforts and ensure security policies and controls are relied upon. The SRB representative(s) coordinating audits shall refer auditors to existing documentation when possible.

3.3.3 Each Agency shall specify a point of contact for media and public information requests involving the RFCS. Requests that involve security controls documentation and PII shall be coordinated among members of the SRB or Agency Security Committee and staff responsible for Public Records Requests.

3.3.4 Agencies shall participate in the ongoing governance processes of the RFCS, including those processes for ongoing development of CDRL 31 Security Plan and enforcement of policy.

3.3.5 Agencies shall conduct day-to-day operations of their business processes for the ongoing RFCS operations in accordance with the security standards and practices adopted by the Joint Board. Agencies shall consider Agency security risks before making major business process changes, and coordinating major changes with other Agencies and the Contractor.

3.3.6 Agencies shall maintain adequate separation of duties among Agency staff operating the RFCS in order to mitigate potential for fraud.

3.4 Asset Management

3.4.1 The Agency Security Committee shall recommend for adoption by the Joint Board a plan for assigning RFCS-related data and records to categories and establishing security and protective measures that are applicable to each category.

3.4.2 The Agency Security Committee shall recommend data export management requirements for adoption by the Joint Board.

3.5 Human Resources and Organizational Security

3.5.1 Each Agency Security Administrator shall assign all User accounts in the RFCS, including computer accounts and accounts on FTP devices, to unique individuals. No accounts will be "shared" among multiple staff.

3.5.2 Each Agency Security Administrator shall notify the Contractor of new User authorizations or removal of existing authorizations with existing employee orientation or termination processes to ensure that they are adopted as standard business practice. Each Agency must specify one primary and one backup Agency Security Administrator who is responsible for sending authorizations and removal notices to the Contractor. Agencies may optionally have additional approval steps prior to this final approval. All access granted will be made on the basis of least privilege. When employment terminates or job responsibilities change, the Agency Security Administrator must promptly notify the Contractor of the account removal or modification.

3.5.3 Each Agency Security Administrator will review User accounts from the RFCS system every quarter. The Agency Security Administrator or another designated individual at each Agency will review a report of accounts and their permissions to verify that all Users remain authorized appropriate to their duties. Any changes must be sent promptly to the Contractor. A positive affirmation that the review has been completed must be provided to the Chair of the Agency Security Committee and to the Security Review Board to document the review.

3.5.4 The Agency Security Administrator for a Lead Agency shall be responsible for requesting from the Contractor unique IDs and passwords for Retail Revalue Entities and Business Accounts with which the Lead Agency is contracting.

3.5.5 The Agency Security Committee will monitor the processes for resetting passwords and managing changes to User accounts and recommend improvements in such processes to the Joint Board.

3.6 Physical and Environmental Security

3.6.1 Each Agency shall restrict physical access to areas that house the Back Office Computer (BOC), Data Acquisition Computer(s) (DAC), and inventory of hardware to only those individuals whose job responsibilities require access and who are documented as being permitted to access those spaces. This access must be restricted using keys or equivalent access systems that limit access to authorized individuals. Documentation must be maintained by each Agency indicating individuals having access to such areas. Each Agency Security Administrator shall review such access lists on not less than a quarterly basis.

3.6.2 Agencies shall ensure that network cabling connected to RFCS network segments is restricted to secure spaces that are not readily accessible from public areas.

3.6.3 Agencies shall ensure that rooms used to house the Back Office Computer and the DACs at each Agency must have an uninterruptible power supply, adequate environmental control such as heating, ventilation and air conditioning capability, and fire suppression.

3.6.4 Agencies must perform an annual inventory of all RFCS equipment that contain Secure Access Modules, including those that are not in production such as training equipment and spare equipment, in order to ensure the equipment is not lost or stolen. The production equipment may be inventoried electronically using communications records; however, non-production equipment must be physically reviewed by an Agency representative. Agencies are responsible for identifying and reporting the theft or loss of a device with a Secure Access Module (SAM) which they control. Agencies must review the Device Connection Report daily on business days, promptly investigate non-reporting devices and report a Security Incident to the Contractor and the SRB within two (2) hours after determining that a device is missing or appears to have been tampered with.

3.6.5 Each Agency must inventory physical device assets when they become Agency property, and apply asset tags or unique identifiers such as a serial number for RFCS equipment.

3.7 Communications and Operations Management

3.7.1 Agencies and the Contractor share firewall configuration responsibilities. Prior to an Agency making changes to firewall configurations that affect Virtual Private Network services or network segregation of the RFCS equipment, the Agency shall first obtain approval by the Agency Security Committee, and then by the Contractor. The Agency shall maintain documentation of the changes. Network traffic traversing the firewall shall be restricted to authorized connections from trusted networks.

3.7.2 Agencies shall provide a network that enables communication from its Back Office Computer to all of its RFCS devices. The RFCS data must be protected from public networks through network segmentation and/or additional data encryption.

3.7.3 Wireless networks which provide RFCS connectivity shall rely on strong levels of encryption.

3.7.4 Agencies are responsible for monitoring and maintaining their network(s). The technologies and processes for monitoring may vary by Agency. Agencies which do not segregate RFCS traffic from other business traffic shall have automated alerts or perform at least weekly reviews of failed log-on attempts to network infrastructure equipment.

3.8 Agency Security Administrator and Access Control

3.8.1 Each Agency shall identify two individuals (a primary and a back-up) to serve as the Agency Security Administrator who shall be responsible for authorizing access to RFCS-related equipment, systems, networks and data. Access to RFCS systems, equipment, networks and data shall be restricted on the concept of least privilege, assigning access only to individuals who have job responsibilities that require such access.

3.8.2 Each Agency will segregate the security access permissions for the individuals having different RFCS roles. The Agency Security Administrator must not have major fiscal or contract administration responsibilities for the RFCS. These

access controls are designed to limit an individual's role to only that which is required to perform their function and an individual acting alone must not have access that could compromise a major aspect of the RFCS. Only the Agency Security Administrator or a designated backup will be authorized to submit changes to user permissions to the Contractor.

3.9 Information Systems Acquisition Development and Maintenance

3.9.1 Agencies shall not perform systems acquisition or development projects that build onto the RFCS without first developing a project plan that addresses feasibility, risks and mitigation strategies, system architecture and security controls, quality assurance and acceptance testing, and implementation to production following review. These project plans must be submitted to the Joint Board or a designated sub-committee for review and coordination, with the purpose of identifying any security controls which are necessary or potential security risks which could result from systems acquisition or development.

3.9.2 When making non-emergency changes to the RFCS that are not initiated by the Contractor, Agencies shall notify the SRB in advance of the Agencies' intention to make such a change, using a designated communication process (such as an e-mail distribution list). The communication should indicate what the scope of the change will be, expected downtime, any test procedures which are planned, and a back-out process. If the change may affect the RFCS components of other Agencies, the change must be coordinated with those Agencies in order to identify risks and mitigate them. Changes which must be coordinated with the Contractor may follow the change management process of the Contractor.

3.10 Agency Security Incident Management

3.10.1 Agencies shall report Security Incidents involving elements of the RFCS which are managed by the Contractor to the SRB, who is responsible for investigation of the incident, coordination of evidence collection, and risk mitigation, according to the ORCA RFCS Data Breach Plan adopted by the Joint Board.

3.10.2 Agencies shall report Security Incidents promptly to the Agency Security Committee.

3.10.3 The SRB must evaluate Security Incidents to determine if an intervention into RFCS configuration is necessary in order to mitigate risk. The SRB will coordinate the activities of the Contractor and Agencies such effort in order to mitigate risk.

3.10.4 If a Security Incident is investigated by an Agency, the Agency must attempt to collect evidence regarding what caused the Security Incident, and if applicable, who was responsible for the Security Incident.

3.10.5 Following the semi-annual report of Security Incidents from the Contractor, or at the discretion of the SRB following a major Security Incident, Agencies shall participate in a post-incident review. The post-incident review must include an open work session to identify the positive and negative elements of a particular incident and identify changes in policy, procedures, or technology controls that could reduce risk in the future.

3.10.6 Subject to public disclosure laws and regulations, public disclosure and communications regarding Security Incidents shall be coordinated among Agencies by the Regional Program Administrator before distributing the information publicly. Issues requiring public communications should be escalated to the Joint Board representative or a designated individual responsible for public information.

3.11 Business Continuity Management

3.11.1 Agencies shall rotate removable back-up media in the Back Office Computer on a schedule defined in coordination with the Contractor.

3.11.2 Agencies shall arrange for the transport of removable back-up media off-site to a secure storage facility at least weekly. Removable back-up media must not be stored in employee homes, automobiles, or unsecured work areas. The off-site facility must restrict physical access to only authorized individuals, and be protected from fire and moisture.

3.11.3 Agencies shall monitor back-up jobs each business day to verify that Back Office Computer back-up jobs are completed successfully. Unsuccessful back-ups must be escalated to the Contractor for problem resolution.

3.12 Compliance and Audit

3.12.1 Through the Regional Program Administrator, Agencies shall be responsible for providing oversight to an annual audit of the Contractor. This audit will verify that the Contractor is performing the principal responsibilities of the CDRL 31 Security Plan and has implemented best practices in the operation of information systems.

3.12.2 The Agency Security Committee shall perform an annual assessment of risk and specify, subject to concurrence by the Joint Board, whether each Agency will perform a self-assessment, have a peer assessment audit, or have an independent audit of compliance with the Agency Security Plan. An independent audit will be performed at least every five years.

3.12.3 To the extent possible, independent audits should be combined with the PCI-DSS audits.

3.12.4 Agencies will be held to the same standard of PCI-DSS compliance as the Agency with the highest volume of transactions and most stringent PCI-DSS compliance requirements. The Agency Security Committee will be responsible for Agency-related PCI-DSS compliance.

3.12.5 An Agency found through an audit not to be in compliance with applicable security requirements will be required to prepare and submit to the Agency Security Committee a remediation plan, including a schedule for achieving compliance. The Agency Security Committee will review such remediation plan and make applicable recommendations to the Joint Board.

4.0 ALLOCATION OF COSTS

4.1 Subject to Joint Board approval, the cost of retaining an outside consultant to conduct an periodic review of the Agencies' compliance with this Plan, including any review of PCI compliance, may be shared among the Agencies. Each Agency shall pay its then-applicable percentage share as provided in the Interlocal Agreement.

4.2 Costs associated with or incurred by an Agency to address deficiencies or compliance issues within that Agency shall be paid entirely by that Agency.

4.3 Costs related to providing staff support to the Agency Security Committee shall be considered Regional Program Administration costs to be funded entirely by the Agency performing Regional Program Administration responsibilities under the Interlocal Agreement.

4.4 Costs related to participating on the Agency Security Committee and providing an Agency Security Administrator shall not be considered to be regional costs and shall be borne exclusively by the Agency incurring such costs.

5.0 AMENDMENTS

5.1 The Agency Security Committee shall monitor the implementation of, and compliance by Agencies, of this Agency Security Plan. If the Agency Security Committee determines that changes to the Agency Security Plan would be in the best interests of the RFCS, it shall submit such changes to the Joint Board for its consideration and action.

5.2 At least annually, the Joint Board shall review the implementation of the Agency Security Plan and consider recommended changes submitted by the Agency Security Committee and proposed changes from other sources. The Joint Board may approve amendments to the Agency Security Plan if such changes would improve efficiency, effectiveness and enhance security of RFCS data and information.

6.0 GENERAL PROVISIONS

6.1 This Agency Security Plan shall be effective on the same date as the Amended and Restated Interlocal Cooperation Agreement of which it is a part.

6.2 The Agencies recognize that time is of the essence in the performance of the provisions of this Agency Security Plan.

6.3 Each Agency shall maintain documentation of its compliance with the provisions of this Agency Security Plan.

6.4 This Agency Security Plan shall be interpreted to be consistent with said Amended and Restated Interlocal Cooperation Agreement. In the event of ambiguities in this Agency Security Plan or inconsistencies between the Agency Security Plan and said Amended and Restated Interlocal Cooperation Agreement, the provisions of said Amended and Restated Interlocal Cooperation Agreement shall prevail.